Safety Assessment Formal Modelling

for Critical Embedded Automotive Sensor-Systems

Jan deMeer
www.smartspacelab.eu
demeer@acm.org

6. Dezember 2006
ASQF FG SW-Testing
Am Borsigturm 20, Berlin-Tegel

Speech Overview

- Avionics On-Board Systems:
  -> IMAC – NSSA – RRA – OIS – FEP
- Avionics Safety Assessment Requirements
  -> Avionics Safety -> HW – SW - Architecure
- Avionics Specification & Design:
  -> V-Model
- Avionics Safety Requirements:
  Modelling - Verification - Testing
- Formal Modelling Languages:
  UML – TLA - Z - TTCN3
- Anticipated Research Contribution on Automotive Systems:
  „AVS" -> „IKT2020"

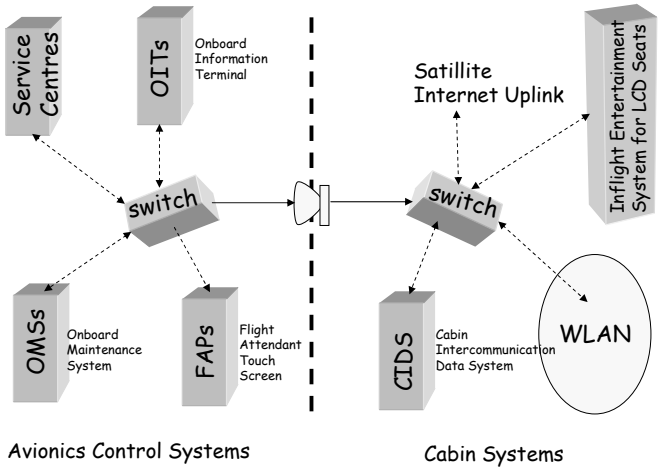
Avionics Notions Refferred to

ACE – Actuator Control Electronics
ACOU – Outlet Unit
AFDX – Avionics Full Duplex Switched Ethernet System
ACUTE – Airbus Cockpit Unversal Thrust Emulator
APU – Auxiliary Power Unit
ARP Aerospace Recommended Practice
DIB – Director Interface Board (Central Board Computer)
EFB – Electronic Flight Bag
E/WD – Engine/Warning Display
FAP – Flight Attendant (LCD Touch Screen) Panel
FbW- Fly-by-Wire
FCGC – Flight Control & Guidance Computer
FCSC – Flight Control Secondary Computer
IMA – Integrated Modular Avionics
IFE – Inflight Entertainment System
KCCU – Keyboard Cursor Control Unit
KID/CID – Configuration- und Identifikation Dokument
MCU – Master Control Unit
MFD – Multifunctional Display
N/SD – Navigation/System Display
NSS – Network Server System
OIS/T – Onboard Information System/Terminal
OMS – Onboard Maintenance System
PFD – Primary Flight Display
RAT – RAM Air Turbine
SFCC – Slat Flap Control Computer
SEB – Seat Electronic Boxes
SAE Society of Automotive Engineering

Integrated Modular Avionics Communication

- Michel Comes, Technical Director of A380 Development Program says: „Delays are due to Compartment Deck Networking Complexity Problems [… with Cables]:
  - 800 passengers in two compartment decks – 560 tons total loads - require light weight construction and materials, e. g.
    - Carbon Fibers, i.e. CFKs
    - Alu wires reduce weight by 300kg!
    - Fly-by-Wire Control Units reduces surface of „Tail Unit Feathers" (Höhenleitwerk) by 40m^2
  - Onboard Integrated Modular Avioncs Communication by AFDX – „Avionics Full Duplex Switched Ethernet Area Network" shares Communication and Computation Ressources, i.e.
    - 100 Mbps Bus – 8 kB Packet Size – 20 I/O Channels per Switch Architecture
    - IMAC Standardization avoids Subsystem Electronic Control Units (HW)
    - IMAC interconnects Subsystems by Twisted Pair Cables
    - IMAC Distributed RT Control Operating System share Hardware
    - IMAC Ressource Sharing hardly applicable for safety-critical Units, i.e. Ressource Reservation Requiring Flight Control Unit

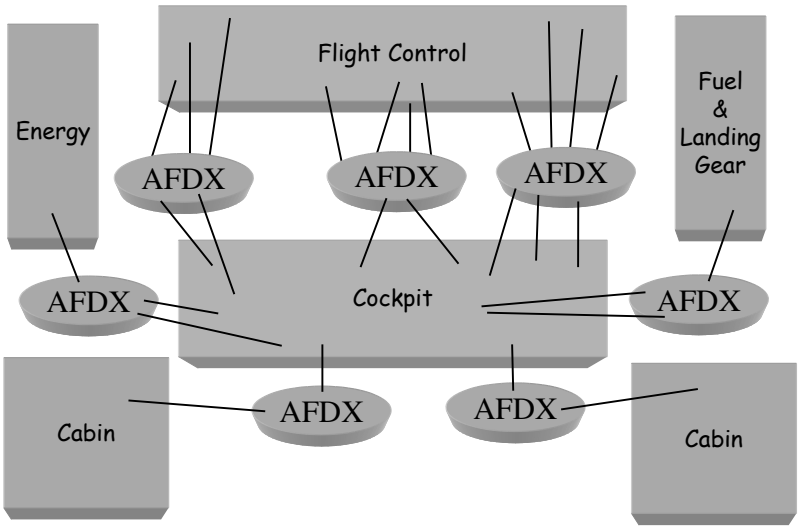
To Obtain Safety by Separation between Cabin and Avionics Control Domains



Network Server System Architecture

- NSS-A separates safety-critical Flight Control Units by dedicated AFDX Area Network (XAN) and separate Power Supply HW, Firewalls to separate Systems, i.e.
  - „Flight Control Domain" comprises Control Units to gear Airplane
  - „Cockpit Domain" comprises Control Units to display and manage I/O from Deck Compartment Subunits, i.e.
    - Keyboard Cursor Control Unit, Primary Flight Display, Navigation Display, Multifunction Display, Onboard Information Terminal, Engine and Warning Display etc.
  - „Power Supply Domain" to supply all Compartment Control Units with electrical power
  - „Fuel Domain", „"Landing Gear Domain" etc.
  - „Passenger Cabin Domain" comprises Sensors/Detectors
    - Controlled One-way Data Flow from Detectors to Cabin Displays only
- Commands from Cockpit Domain are supervised by NSS Flight Control and Guidance Computer and finally forwarded to Plane Actuators

NSS Ressource Reservation Architecture



Onboard Information System

- „Electronic Flight Bag" := OIB
-
  - OIS-Data Loaded by CD, USB, WLAN from Airport Briefing Centre
  - OIS Comprises
    - Navigation Maps,
    - Airport Maps including Airplane Position
    - Airplane User Manuals, Logging Books
    - Computation of Centre of Gravity during Loading
    - Update with Current Cabin Conditions of Temperature, Pressure, Onboard Maintenance System, Fly-by-Wire Parameters

OIS - Actuator Control Electronics

- Digital vs. Analog Flight Control
  - Translation of Analog Pilot Sidestick Movements into Digital Signals forwarded by the NSS Flight Control and Guidance Computer to the Plane Actuator
  - Airbus A380 has 8 FCG Computers of following Priority to minimize Safety-critical Failures:
    - 3 Primary FC GC (Quer- u. Höhenruderkontrolle)
    - 3 Secondary FC SC
    - 2 Slat Flap (Vorflügel u. Landeklappen) Control Computer SF CC
  - Each of these Computers has a Command and a Monitoring Unit COM/MON
  - Double Checked by Control Units on Measurements and Runtime System Failures to keep Airbus FbW-Functioning

OIS – Flight Envelope Protection

- Keeps Aircraft Cruise Control by Using
  - Air Data Inertial Reference Units, i. e. ADIRU DB
  - 3 System States: Normal – Alternate – Direct
    - Normal Law: FEP has complete control over Pilot's Actions
    - Alternate Law: FEP has partial Control over Pilot's Actions
    - Direct Law: FEP has almost no Control over Pilot's Action
  -

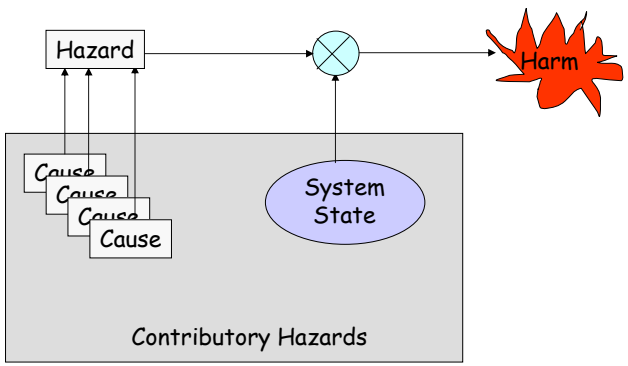
OIS - Inflight Entertainment System

- By Thales: „TopSeries i-5000" On-Demand System
  - Gigabit Ethernet Connection with 5 Mbps/Guest with „Leaky Line" WLAN Access
  - Area Distribution Boxes translate MPEG-5 streams
  - GSM/GPRS Mobile (Handy) Telephony
- By Panasonic Avioncs: „eX2" System
- Digital Cabin Intercommunication Data System
  - Cabin Parameter Control by
    - Control Computer „Director"
    - Director Interface Board DIBs
    - Flight Attendant Panels FAPs
    - TCP/IP Network

„Airborne Safety Assessment"

- Safety Engineering, as suggested by Federal Aviation Administration
- FAA Order 8040.4 – Safety Assessment Process on Civil Airborne Systems
- Hazard Analysis: Severity & Likelihood of Occurrance
  - Category of „initiating" Hazard involves System Environment Conditions
  - Category of „contributing" Hazard involves System States, Failures, Malfunctions
  - Accident Scenario to analyse risk of harm due to hazards

FAA Safety Engineering – Accident Scenario



„Airborne Safety Assessment"

- SAE ARP 4761: „Guidelines and Methods for Conducting the Safety Assesement Process on Civil Airborne Systems and Equipment"
- SAE ARP 4754: „Certification Considerations for Highly Integrated Complex Aircraft Systems" ~ „Airborne V-Model"
  - Specifications Related:
    - RTCA DO178B SW Considerations
    - RTCA DO254 HW Considerations
      - S/H ware Development Assurance Levels:
      - Effect of Anomalous Behavior: A(catastrophic) – E(no effect)
  - Procedures
    - Functional Hazard Assessment
    - Preliminary System Safety Assessment
    - System Safety Assessement
    - Common Cause Analysis
  - Analytical Approaches
    - Fault Tree Analysis
    - Failure Mode Effects Analysis/Summary
    - Dependency Diagrams
    - Markov Chain Analysis

FAA Aquisition Management System Process: Safety Definitions

- Catastrophic := Multiple Fatalities, Loss of System
- Hazardous := Reductions on System/Operator Capabilities to Extent of
  - Large Reduction in Safety Margin
  - Operators cannot perform Tasks or Functions Accurately or Completely
  - Serious or Fatal Injury to small Number of Occupants eycept Operator
- Major := Reductions on System/Operator Capabilities to Extent of
  - Significant Increase in Operator Workload
  - Physical Distress to Aircraft Occupants, except Operator
  - Major Occupational Illness, Environmental or Property Demage
- Minor := Does not Reduce Significantly System Safety; Operator's Action are within Capabilities including
  - Slight Increase of Workload,
  - Physical Discomfort to Occupants, Aircraft, except Operator

FAA AMS Process: Safety Likelihood

- Probable := to occur 1 or more times during entire Operational Lifetime of an Item
  - Probability > 10^{-5}
- Extremely Remote := to occur several times of an entire System (Fleet)
  - Probability > 10^{-7}
- Remote := to occur few times of an entire System (Fleet)
  - Probability > 10^{-9}
- Extremely Improbable := Unlikely to Occur during entire Operational Lifetime of an Entire System (Fleet)
  - Probability per Operational Hour < 10^{-9}

FAA AMS Process: Severity of Consequences and Likelihood

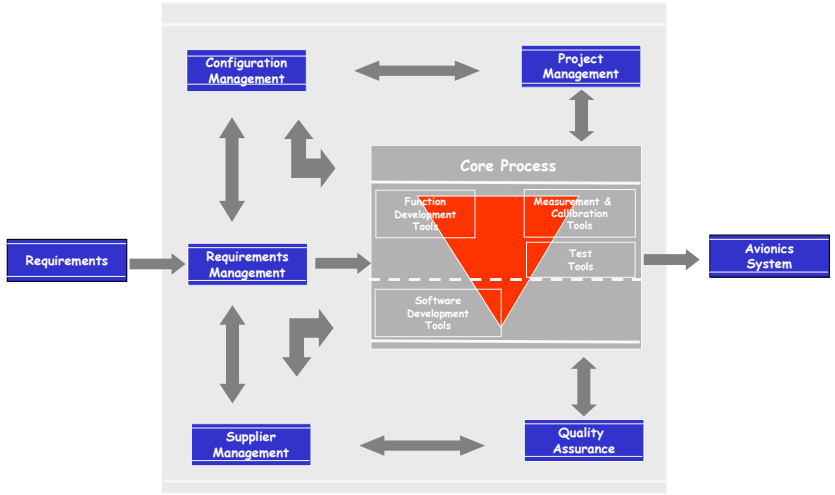
- Category 1 „Catastrophic" := Death, System Loss, Severe Evironmental Demage
- Category 2 „Critical" := Severe Injury, Occupational Illness, Major System/Environmental Demage
- Category 3 „Marginal" := Minor Injury, Occupational Illness, Major System/Environmental Demage
- Category 4 „Negligible" := Less than minor Injury, Occupational Illness, S/E Demage

ATEM V-Model:

The V-Model – Standards

- VM by Graphical Development Process Assistant for IT Systems (VM'97)
  - General Directive No. 250: Process Model
  - General Directive No. 251: Methods Allocation
  - General Directive No. 252: Functional Tool Requirements
    - VM by ANSSTAD – Anwender SW Standard der Öffentl. Verwaltung www.ansstad.de
    - VM by IABG Industrieanlagen Betriebsgesellschaft
  - GD250 Configuration Management with Hierarchical Levels of Systems
    - System/SW/HW Configuration Identification Documents
    - Technical System Architecture/Structure
    - Identification of Interfaces
    - Requirements Allocation
    - Solution Proposal, e.g. SW Architecture
    - Feasibility Studies
    - IT Security Concept and Model

The V-Model – Graphical Developement - GD 250 Standard



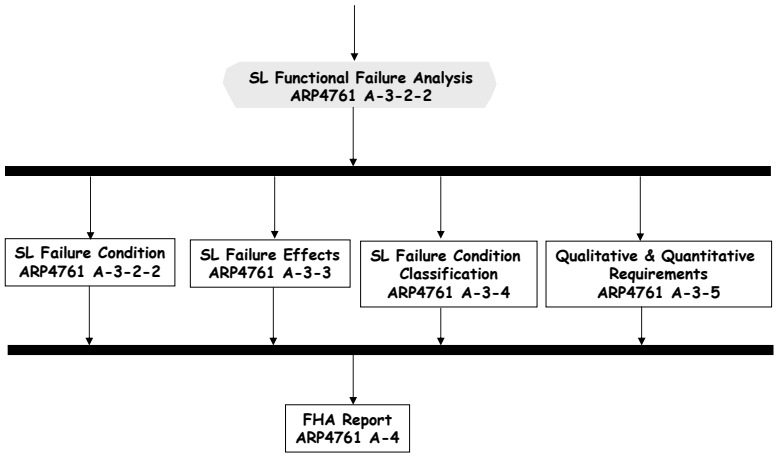
Life Cycle Process Model with UML

- ViSEK Project by UoOldenburg (2003)
- Goal: ARP4754 Integration into VM'97
- Objective: To Gain a Unique Process Modelling Languages Domin-independent
  - Graphical Representations by UML Modelling Notions
    - Constraints, Properties by Language for Metamodels (Meta-Metamodel)
    - Operations, Attributes by Language for Metamodel Instances
    - Object Classes by Language for Information Domain
    - Object Class Instantiation of Information Domain

Life Cycle Process Model with UML

- Mapping of static and dynamic VM Notions into UML
  - GD250 Activity Schema |-> UML Classes/Transitions
  - Aerospace Recommended Practice 4754/4761 for Safety Assessment includes
    - Functional Hazard Assessement „to classify" Failures
    - (Preliminary) System Safety Assessment „to verify/test" at System Level implemented Safety Requirements
    - Common Cause Analysis „to verify/test" System Component Autonomy (Independence) to obtain System Safety Needs

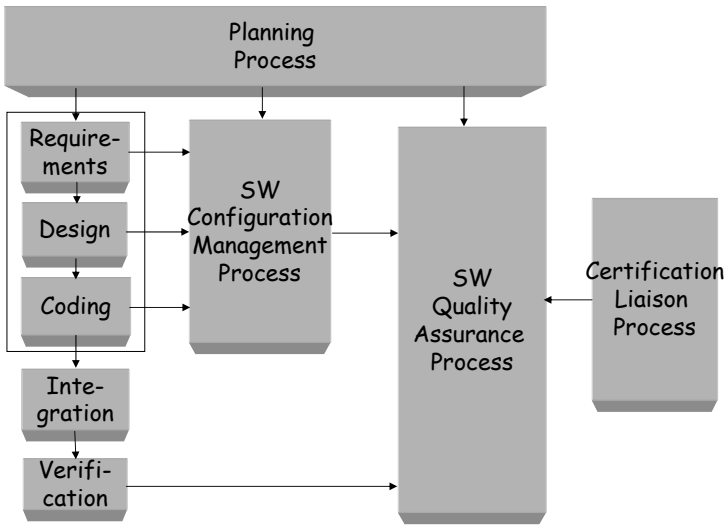
VM UML Example: FHA Detailled Activity Description



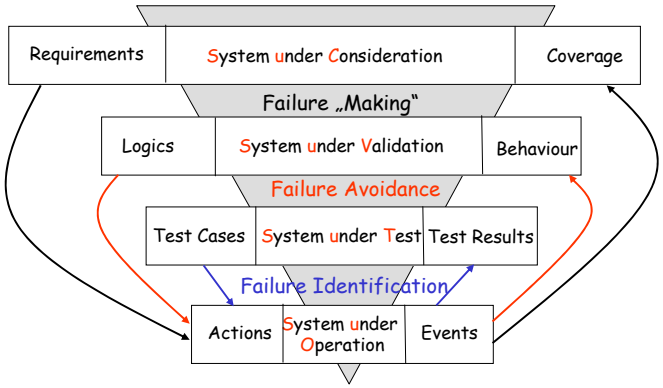
Airborne - DO178B - SW Constraints

- Plan for SW Aspects and Certification PSAC
- SW Development Plan (SDP)
- SW Verification Plan (SVP)
- SW Configuration Management Plan (SCMP)
- SW Quality Assurance Plan (SQAP)
- SW Requirements Standards (SRS)
- SW Code Standars (SCS)
- SW Design Description (SDD)
- Source Code (Data File)
- Executable Object Code (Data File)
- SW Verification Cases and Procedures (SVCP)
- SW Verification Results (SVR Records)
- SW Life Cycle Configuration Index (SECI)
- SW Configuration Index (SCI)
- Problem Reports (PR Records)
- SW Configuration Management Records (SCMP Records)
- SW Quality Assurance Records (SQAP Records)
- SW Accomplishment Summaries SAS

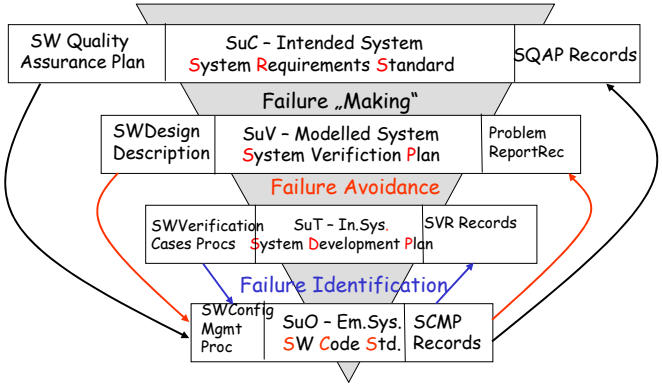
PSAC Life Cycle Model



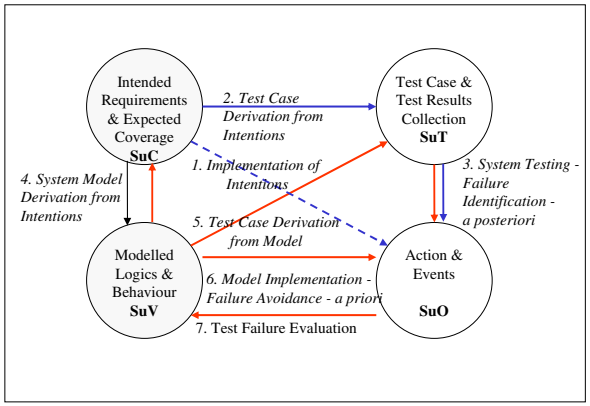
The ATEM V-Model – „QoS Engineering"



The ATEM V-Model – DO178B Engineering



The ATEM V-Model - QoS Relationships



"Verification" by Testing

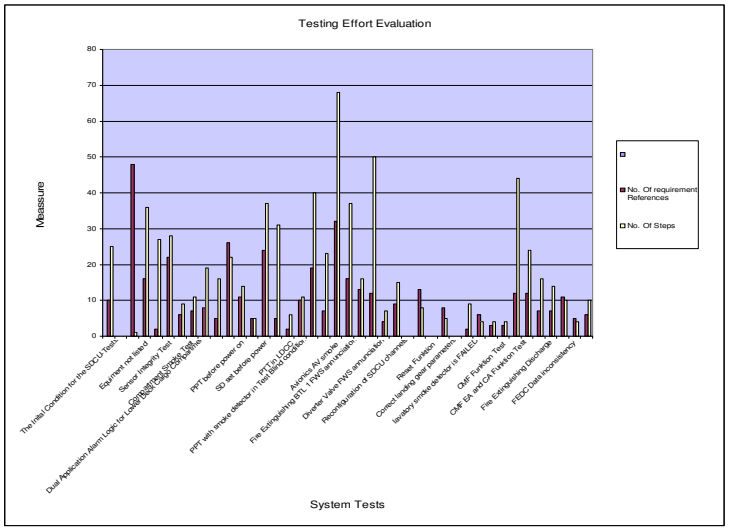
QoS Requirements from Customer

- „Correctness Proof" of Innovative Technology for Airbus Passenger Cabins
  - High Degree of Complexity of SuT Behaviour and Architecture
  - „Measuring" of Critical Constraints
    - Quality of Service (QoS) Constraints:
      - „How to recognize events and react on in real-time?
      - „How does the system react on congestion and contention conditions?
    - Reliability:
      - Robustness: „tolerance against failures"
      - Safety:
        - » „nothing bad will happen"
        - » „Expected events eventually will happen"
    - Secrecy:
      - Exclusive Informaton Exchange
      - Information Integrity

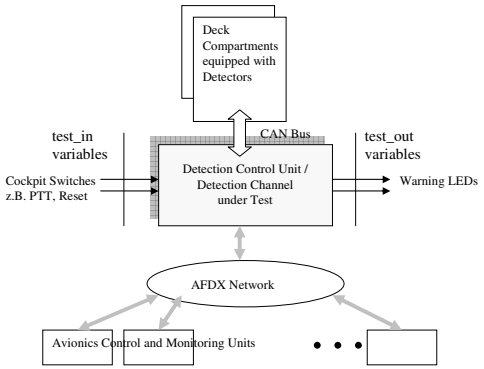
How to „Approve Correctness" of Critical QoS Requirements?

- Degrees of System Correctness Achievements:
  - Highest: Proof with Formal Methods Existence or Absence of Constraints on System Behaviour
    - Consistency: System Features do not contradict
    - Completeness: There is no feature that has not been considered by the proof.
    - Examples: Model Checking, Z-Method, Formal Process Calculi, Derivation Systems, ...
  - Medium: Proof with semiformal Testing Methods
    - Incompleteness: Absence of Failures cannot be tested
    - Inconclusive Semantics: Heterogeneous Methods, e.g. „Tree-and Tubular-combined ..."
    - Comparable Results/Evaluations because of Standardized Methods
    - Examples: FDTs, TTCN, UDL,
    - ...
  - Low: Proof with Proprietary Methods:
    - Incomplete: Testing is incomplete
    - Inconclusive: most tools obey partial non-formal semantics
    - Non-Comparable: Do same test cases applied to different System Features obey with the same (observational) semantics? (hard to assess)

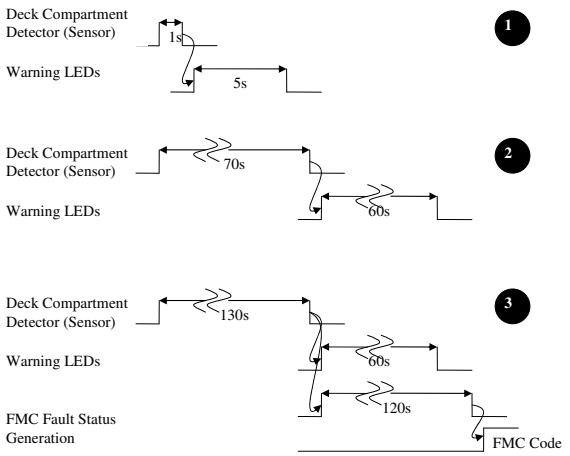
„Airborne Test Case Complexity"



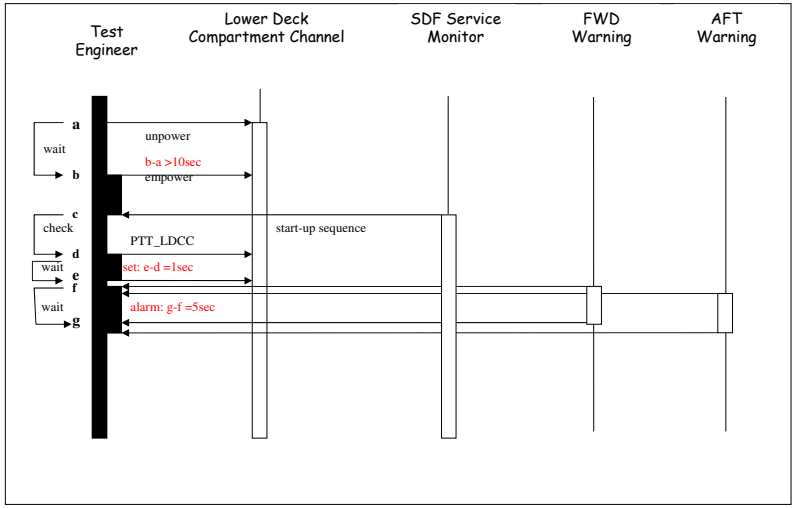
Airborne Test Case for IMA Shared Ressources Architecture



Hazard Test Case Specification: Harmless – Critical – Hazardous Failure



Hazard Test Case Specification – UML Interaction Diagram Sample

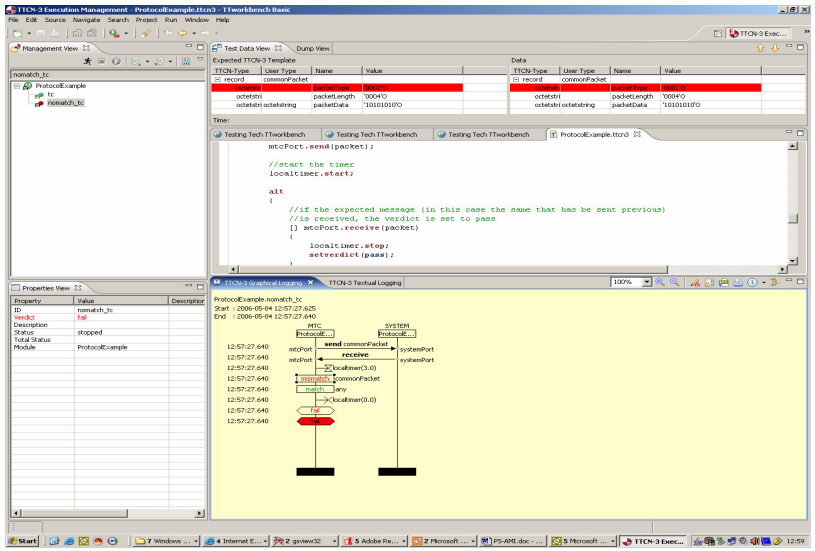


Hazard Test Case Specification TTCN3 Sample:

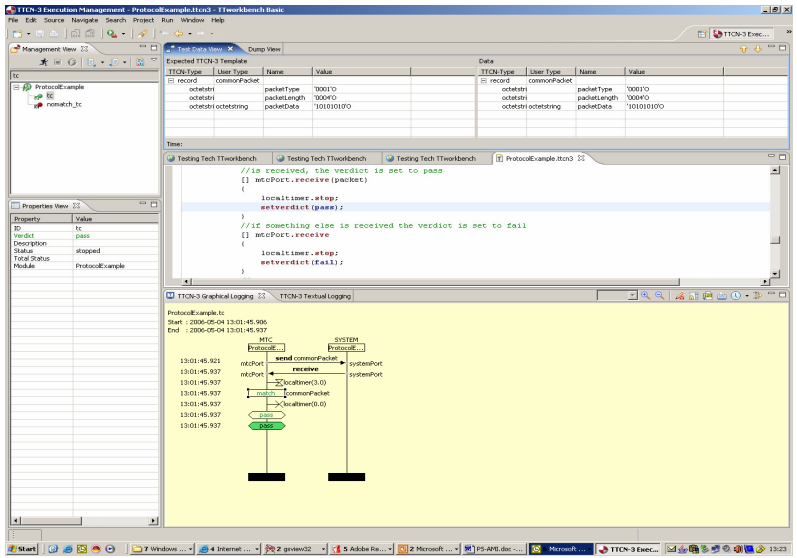
```
timer harmlos_mldg := 1.0;
timer kritisch_mldg :=  70.0;
timer gefährlich_mldg := 130.0;
timer harmlos_alarm := 5.0;
timer kritisch_alarm := 60.0;
timer gefährlich_alarm := 60.0;
```

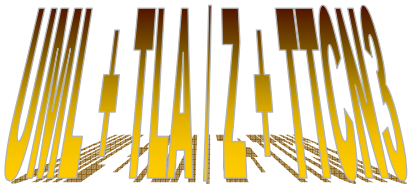
```
Testcase: harmlose_Meldung () runs
    on PTT_Tester {
// Timing Conditions:
timer harmlos_mldg := 1.0;
timer harmlos_alarm := 5.0;
    // PTT Tester Stimulation by
    Actions:
ldcc_in.send (GND);
    harmlos_mldg.start;
    harmlos_mldg.timeout;
    // SUT Reaction by Observations:
ldcc_out.receive (FWD, AFT);
    fmc_out.receive ("code")
    harmlos_alarm.start;
    harmlos_alarm.timeout;
    setverdict( pass );
};
```


TTCN3 TestingTech-Tooling Sample: „Fail" Operation



TTCN3 TestingTech-Tooling Sample: „Pass" Operation





UML Diagrams

Aktivitätsdiagramme: Kontrollfluß

Use Case Diagramme: Interaktionen zwischen systemexternen Nutzern, sog. Aktoren, und dem System selbst

Sequenzdiagramme: temporalen Abhängigkeiten (vgl. Aktivitätsdiagramm) von Ereignissen oder Aktivitäten

Collaboration Diagramme: Interaktionsbeziehungen zwischen Systemkomponenten oder Aktoren, sog. UML-Objekte

Klassendiagramme: Gemeinsamkeiten von Objekten. Objektstruktur (Attribute), Objektverhalten (Operationen) und Objektrelationen

Beziehungen, bzw. Relationen zwischen den Objektklassen, d.h. *association, aggregation, dependency, inheritance.*

Zustands/Transitions Diagramme: Ursache (externes Ereignis) und Wirkung (Systemtransition), d.h. (dynamisches) Verhalten von Objektklassen

Komponentendiagramme: Architektur, bzw. Organistionsstruktur eines Systems, z.B. Schnittstellen zwischen Softwarekomponenten

Deployment Diagramm: Einbettung des beschriebenen Systems in die Nutzungsumgebung;

Stereotyp Diagramm: Systemdarstellung offen für semantische Ergänzungen zu lassen, z.B. Stereotype für „distrubution"-Konzept, das es explizit in der aktuellen UML-Version (noch nicht) gibt.

Standardized Testing Methodologies

- TTCN3 – Standardized and Maintained by ETSI
  - Origin: ISO/IEC 9646: OSI Conformance Testing Methodology early in the 1980ies
  - Nowadays: ETSI Method for Testing and Specification comprising 6 parts:
    - Core Language (Part 1)
    - Tabular Presentation Format TFT (Part 2)
    - Grafical Presentation Format GFT (Part 3)
    - Operational Semantics (Part 4)
    - Runtime Interface TRI (Part 5)
    - Control Interface TCI (Part 6)
  - Experienced by huge testing community
    - Work Bench (Tools) by Industry, SMEs
    - Methodology by Research & Standardization Groups
    - National/International User Groups, e.g. ASQF (Germany)

Temporal Logics of Actions TLA+

Seien A und B Aktionsschritte, e der Wert eines Aktionsschrittes und F, G sind Aussagen, bzw. temporale Bedingungen für eine Aktion, dann bedeuten:

- e' [Wert e am Ende eines Aktionsschrittes];
- $[A]e$ $[A \vee (e'=e)]$,
- d.h. der Aktionsschritt A ist ausgeführt oder der Aktionswert ist gleich e;
- $\langle A \rangle e$ $[A \wedge (e' \neq e)]$,
- d.h. der Aktionsschritt A ist ausgeführt und der Aktionswert ist ungleich e;
- ENABLED A [Aktionsschritt A ist möglich];
- UNCHANGED e $[e'=e]$;
- $\Box F$ [F ist (von jetzt an) immer wahr];
- $\Diamond F$ [F wird (an einem späteren, unbestimmten Zeitpunkt) wahr werden];
- WF$_e(A)$ [Voraussetzung, daß Aktion A eintritt, ist schwach-fair];
- SF$_e(A)$ [Voraussetzung, daß Aktion A eintritt, ist stark-fair];
- $F \rightsquigarrow G$ [wenn F eintritt, folgt G];
- $F \mapsto G$ [wenn F eintritt, ist G garantiert];
- $\exists x: F$ [Aussage x ist implizit in F enthalten (hiding)];
- $\forall x: F$ [Aussage x ist explizit in F enthalten (generalization)];

FDTs applied for CIDS Assessment

HYBRIS – Integration of SW Specification Techniques for Scientific Engineering Application, www.informatik.uni-bremen.de/~jp/hybris.html

VICTORIA – Design Methods for New Generation of Commercial Aircraft Electronic Systems, i.e. Onboard Information Systems, Integrated Modular Electronics, Thales Avionics 2004

Graphical Methods and Tools for Test Specifications based on Timed CSP to be applied to HW-in-the-loop Testing of Aircraft CIDS, Jan Peleska et al. UoBremen 2003

AIRBUS-ASTS – Automatic HW-in-the-loop Test System for Daimler-Chrysler Aerospace Airbus CIDSystems, Jan Peleska et al. 1999

AIRBUS-CIDS – Test and Verification of CIDS SW by using FDTs, H-M. Hörcher, J. Paleska SW Quality Journal 4, 309-327 (1995)

BMBF IT Forschung „IKT2020"

- 4.2 SW Systeme: http://www.it2006.de/de/175.php
  - Themen:
    - SW Engineering,
    - Mensch-Technik Interaktionen
    - Intelligente Systeme / Wissensverarbeitung
  - SW Engineering
    - Embedded Systems – von Einzelsystemen zu vernetzen Systemen
  - Steigerung der SW Entwicklungsproduktivität durch Forcierungen am
    - Prozeß der „Leistungsgestaltung" (Paradigma SW Engineering)
    - Prozeß der „Leistungserbringung" (Paradigma SW Produktion)
  - Forschungsthemen
    - Prozesse, Werkzeuge, Methoden für sicherheitskritische, eingebettete SW Systeme
      - Durchgängiges Referenzmodell für die Formale Programmentwicklung (Spezifikation – Transformation – Verifikation)
      - Verifzierbare (Testbare) echtzeitfähige Anwendungskomponenten
    - Empirische Erprobung von Techniken, Werkzeugen auf Eignung bestimmter Anwendungsgebiete, z.B. Avionics

Conclusions

- Problem: Safety Assessement of Complex Autonomous Sensor Systems
- Goal: Airborne V-Model „to assess formally" Safety Requirements at Autonomous Distributed Systems (Autonome Verteilte Systeme), i.e. Aircraft CIDS
- Work Plan: ATEM Research Project Plan on Avionics Test and Evaluation Platform
- SME Contributions?


Fin - merci beaucoup, Jan